(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number : **0 536 943 A2**

(12) EUROPEAN PATENT APPLICATION

(21) Application number : 92308939.5

(22) Date of filing : 30.09.92

(51) Int. Cl.^{5} : **G06F 12/14**

(30) Priority : 11.10.91 GB 9121591

(43) Date of publication of application :
14.04.93 Bulletin 93/15

(84) Designated Contracting States :
AT BE CH DE DK ES FR GB GR IE IT LI LU MC
NL PT SE

(71) Applicant : Pilkington Micro-Electronics Limited
Prescot Road St. Helens
Merseyside WA10 3TT (GB)

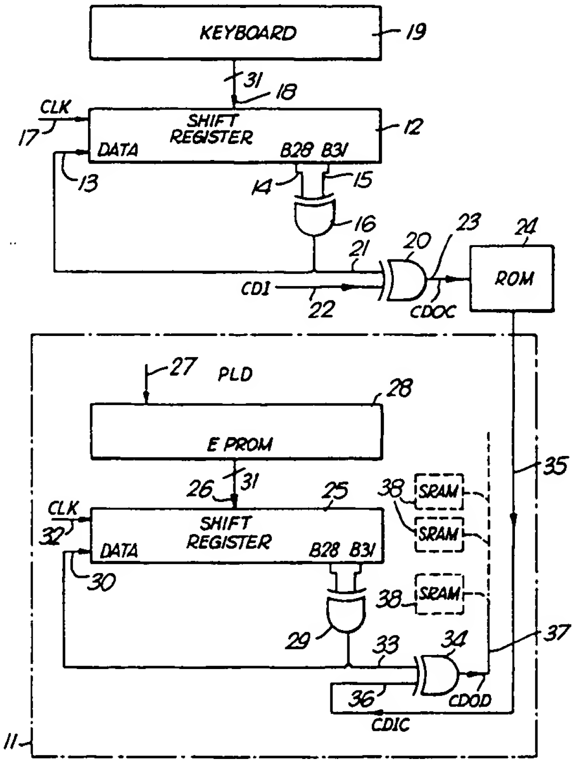
(72) Inventor : Austin, Kenneth
Brockhurst Hall, Brockhurst Way
Northwich, Cheshire CW9 8AP (GB)

(74) Representative : Palmer, Roger et al
PAGE, WHITE & FARRER 54 Doughty Street
London WC1N 2LS (GB)

(54) Data security arrangements for semiconductor programmable logic devices.

(57) A data security arrangement is provided to protect configuration data to be stored in static random access memories (38) in semiconductor programmable logic devices PLD. The configuration data, which is vulnerable to illegal duplication, is normally held in a read only memory ROM, typically an erasable programmable read only memory.

A data coding means is provided to code the configuration data to be loaded to the PLD and a data decoding means is provided in the PLD to decode the coded configuration data. The coding and decoding means each incorporate maximal length shift registers (12, 25) which generate a pseudo-random sequence of bits. A key value is input to the shift register (12) in the coding means forcing it to start at a particular point in the sequence. The output (bits B28 and B31) of this register is combined in an EXCLUSIVE-OR gate (20) with configuration data and coded data is written to the read only memory ROM (24). The decoding means in the PLD has a corresponding key value held in a non-volatile memory (28) in the PLD. This is applied to the register (25) of the decoding means whose output (bits B28 and B31) are combined in an EXCLUSIVE-OR GATE (34) with coded configuration data CDIC read from the ROM (24) to produce decoded configuration data CDOD to be sotred in the memories (38).



EP 0 536 943 A2

Jouve, 18, rue Saint-Denis, 75001 PARIS

The present invention relates to data security arrangements for semiconductor programmable logic devices.

The invention finds particular utility in semiconductor programmable logic devices (PLDs) of the type including an associated storage means e.g. a static random access memory (SRAM) in which circuit configuration data, necessary for the device to operate, is retained.

It is well known that prior to a PLD being loaded with appropriate circuit configuration data, such data is normally held in an external storage medium e.g. an erasable programmable read only memory (EPROM). A disadvantage of the present circuit configuration data loading arrangements to the PLD is that a copy can be readily taken and as a consequence valuable and sensitive circuit information can be easily and illegally duplicated. It is extremely desirable, therefore, to protect circuit information from being copied.

An aim of this invention is to overcome this disadvantage by the provision of a data security arrangement for loading configuration data which prevents illegal duplication of such circuit information.

According to the present invention, there is provided a data security arrangement for a semiconductor programmable logic device comprising data coding means, first storage means, and incorporated within the programmable logic device, data decoding means together with associated second storage means, wherein the data coding means codes originating operating data, and the first storage means stores the coded originating operating data and wherein the data decoding means decodes the coded originating operating data read from the first storage means into the originating operating data form prior to loading to the associated second storage means.

Preferably the data coding means and the data decoding means each include a pseudo-random sequence generator constituted by a 31-bit maximal length shift register having a preload input and a DATA input, the shift register generating a pseudo-random sequence equivalent to 2,147,483,647 bits in overall length.

Preferably bit 28 and bit 31 outputs of the maximal length shift register are input to an EXCLUSIVE-OR logic function whose output is connected to the DATA input of the maximal length shift register.

The maximal length shift register is preferably forced to start the pseudo-random sequence at a particular point in the sequence by the application of a predetermined sequence start code constituted by a 31-bit "key value" to the preload input.

The application of the sequence start code to the maximal length shift register in the data coding means may be input from a keyboard or from a secure file, whereas the application of the sequence start code to the maximal shift register in the data decoding means is preferably input from a non-volatile memory within the programmable logic device.

The data employed to enable the programmable logic device to operate is preferably circuit configuration data and it is arranged in the data coding means for the circuit configuration data and the pseudo-random sequence to be input to an EXCLUSIVE-OR logic function to provide an output of coded circuit configuration data.

Preferably in the data decoding means the pseudo-random sequence and the coded circuit configuration data are input to an EXCLUSIVE-OR logic function to provide an output of decoded circuit configuration data.

The first storage means may be constituted by a read only memory, whereas the associated second storage means is constituted by static random access memories.

The invention will be more readily understood from the following description of an exemplary embodiment which should be read in conjunction with the accompanying drawing.

The drawing illustrates a block schematic circuit diagram of the data security arrangements in accordance with this invention.

Referring to the drawing, a programmable logic device 11 is represented by the block designated PLD. To facilitate security of data loaded to the PLD, a data coding means is provided to code circuit configuration data, termed originating operating data, which is to be loaded to the PLD, and similarly a corresponding data decoding means is provided in the PLD to decode the coded circuit configuration data in the PLD.

Referring to the data coding means in more detail, a particular form of shift register 12 is provided which generates a maximal length pseudo-random output string. This type of shift register is known as a "maximal length shift register" and in the present application the overall length of the pseudo-random sequence is arranged to be equivalent to 2,147,483,647 bits (see CMOS COOK BOOK by Don Lancaster pages 318-323, published by Howard W Sams Corp 1980).

This is achieved by feeding back to a DATA input 13 of the register, particular outputs 14 and 15 of the register in a particular manner. In this instance both outputs 14, 15 which provide bits B28 and B31 are input to an EXCLUSIVE-OR gate 16 and the output of this gate is input to the DATA input 13. Providing the register 12 is continuously driven by a clock input signal 17, the generated pseudo-random sequence is continuously repeated.

In the data coding means the register 12 is preloaded (in parallel form) with a predetermined one of different "key values", each of 31 bits, typically input to a preload input 18 by way of a keyboard 19 or alternatively from a secure file. The "key value" which may be termed a sequence start code, forces the shift register 12 to start the pseudo-random sequence at a particular point in the sequence and thereby recreate an identical sequence at any time as required.

The pseudo-random sequence output from the EXCLUSIVE-OR gate 16 is input at 21 to a further EXCLUSIVE-OR gate 20. Circuit configuration data CDI (generated from circuit configuration layout software) which is to be coded is input at 22 to the gate 20. The output 23 from the EXCLUSIVE-OR gate 20 generates coded circuit configuration data CDOC.

The coded circuit configuration data CDOC is output from gate 20 to a first storage means 24, typically, a read only memory, where it is held until required by the programmable logic device 11. The circuit configuration data now stored in the first storage medium 24 is coded and secure, and if copied in this form would not yield any useful circuit information to the data copier.

To make use of the circuit configuration data in the programmable logic device 11 when it is read from the first storage medium 24, the data needs to be reproduced in its original form and this is achieved by data decoding means.

The data decoding means is required to regenerate the same pseudo-random sequence of bits as was employed in the data coding means. Accordingly, the programmable logic device 11 incorporates a 31-bit maximal length shift register 25 of the same form as the register 12 employed in the data coding means.

For decoding to be accurate and effective the shift register 25 must commence its pseudo-random sequence at the corresponding point at which the shift register 12 commenced its sequence. Accordingly the identical predetermined 31-bit "key-value" or sequence start code which was used to start register 12 must be applied, in parallel form, to a preload input 26 of the register 25 to force it to start its sequence at the same point in the sequence as register 12, and thereby genrate an identical paseudo-random sequence.

The required 31-bit "key value" is input at 27 and stored in a form of non-volatile memory on the PLD 11, for example, an EPROM 28 or fusible links.

The shift register 25 operates in a manner similar to shift register 12, the output bits B28 and B31 being input to an EXCLUSIVE-OR gate 29 whose output is fed to the DATA input 30 of the register. The register 25 is driven by the clock signal CLK input at 32.

The pseudo-random sequence output from EXCLUSIVE-OR gate 29 forms an input 33 to a further EXCLUSIVE-OR gate 34 and coded circuit configuration data CDIC which is output from the first storage means 24 on line 35 forms a second input 36 to the gate 34.

The EXCLUSIVE-OR function of the gate 34 upon its two signal-inputs produces an output 37, in serial form, of the originating operating data (the circuit configuration data). This originating operating data is now available for use within the programmable logic device PLD, for instance, loading into associated second storage means in the form of static random access memories SRAM 38.

Claims

1. A data security arrangement for a semiconductor programmable logic device (11) characterised by the data security arrangement comprising data coding means, first storage means (24), and incorporated within the programmable logic device (11), data decoding means together with associated second storage means (38), wherein the data coding means codes originating operating data (22), and the first storage means (24) stores the coded originating operating data (23) and wherein the data decoding means decodes the coded originating operating data (35) read from the first storage means (24) into the originating operating data from (22) prior to loading to the associated second storage means (38).

2. A data security arrangement as claimed in claim 1, wherein the data coding means and the data decoding means each include a pseudo-random sequence generator.

3. A data security arrangement as claimed in claim 2, wherein the pseudo-random sequence generator is constituted by a 31-bit maximal length shift register (12,25) which generates a pseudo-random sequence equivalent to 2,147,483,647 bits in overall length.

4. A data security arrangement as claimed in claim 3, wherein the maximal length shift register (12,25) has a preload input and a DATA input.

5. A data security arrangement as claimed in claim 4, wherein bit 28 and bit 31 outputs of the maximal length shift register (12,25) are input to an EXCLUSIVE-OR logic function (16,29) whose output is connected to the DATA input of the maximal length shift register (12,25).

6. A data security arrangement as claimed in claim 4 or claim 5, wherein the maximal length shift register (12, 25) is forced to start the pseudo-random sequence at a particular point in the sequence by the application of a predetermined sequence start code constituted by a 31-bit "key-value" to the preload input (18,26).

7. A data security arrangement as claimed in claim

6, wherein the application of the sequence start code to the maximal length shift register (12) in the data coding means is input from a keyboard (19) or from a secure file.

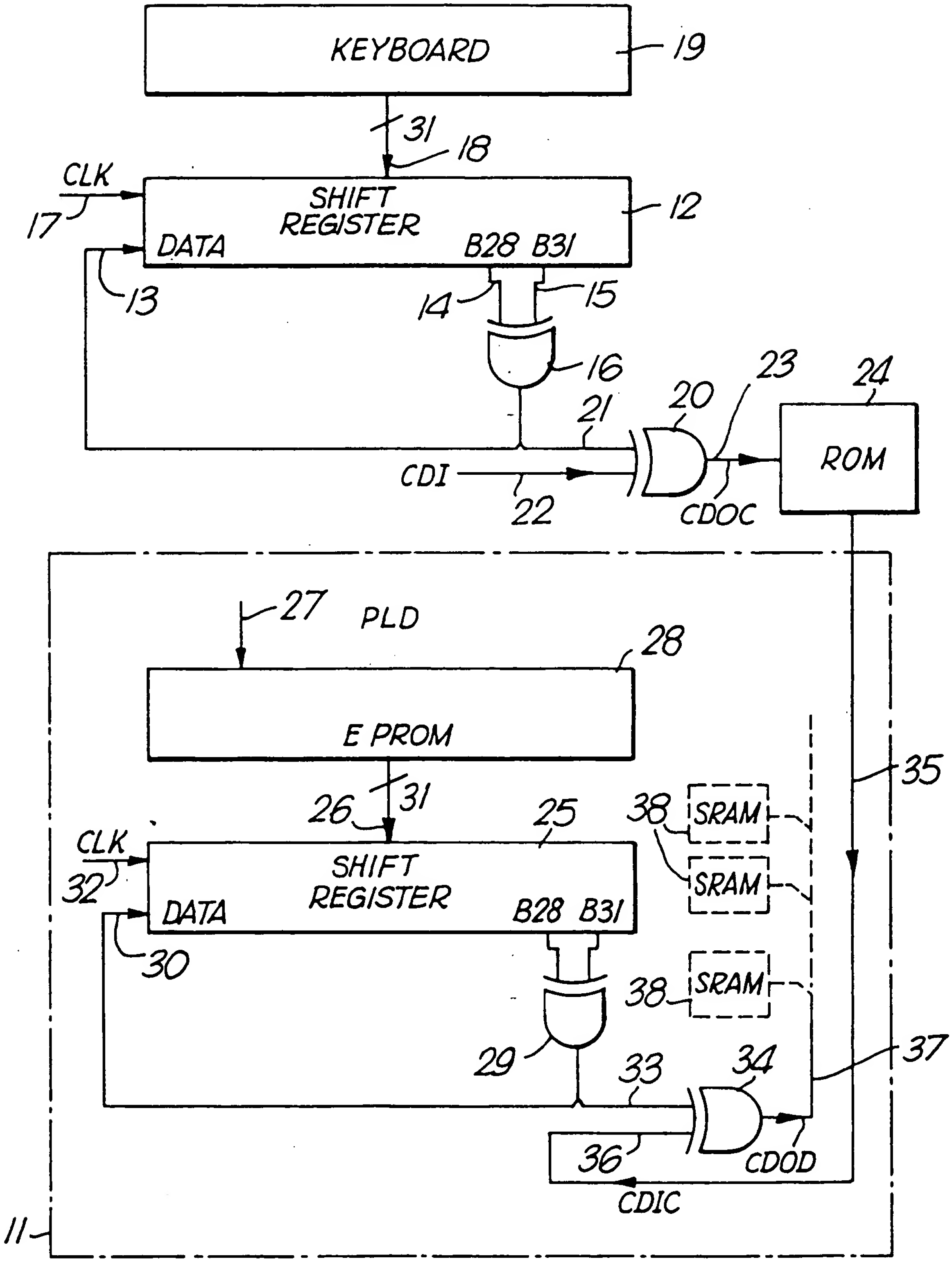
8. A data security arrangement as claimed in claim 6 or claim 7, wherein the application of the sequence start code to the maximal shift register (25) in the data decoding means is input from a non-volatile memory (28) within the programmable logic device.

9. A data security arrangement as claimed in any one claim from claim 3 to claim 8, wherein the originating operating data (22) is circuit configuration data and wherein in the data coding means the circuit configuration data and the pseudo-random sequence are input to an EXCLUSIVE-OR logic function (16,20) which outputs coded circuit configuration data.

10. A data security arrangement as claimed in claim 9, wherein the pseudo-random sequence and the coded circuit configuration data (35) are input to an EXCLUSIVE-OR logic function (29,34) in the data decoding means to provide an output of decoded circuit configuration data.

11. A data security arrangement as claimed in any one preceding claim, wherein the first storage means is constituted by a read only memory (24).

12. A data security arrangement as claimed in claim 11, wherein the associated second storage means is constituted by static random access memories (38).


KEYBOARD
19
31
18
CLK
17
SHIFT REGISTER
DATA
B28 B31
12
13
14
15
16
21
20
23
24
ROM
CDI
22
CDOC
27
PLD
28
E PROM
31
26
25
38
SRAM
SRAM
35
CLK
32
SHIFT REGISTER
DATA
B28 B31
30
38
SRAM
29
33
34
37
36
CDOD
CDIC
11